

NetStalker and HP Open View

| Claim number | Claim Term | NetStalker (public use/on sale) | HP Open View (printed publication and public use) |
|--------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 203 | | | <p>set to:</p> <ul style="list-style-type: none"> • Do not pass status up • Pass status up one level • Pass status up all levels" (4-18) [SYM_P_0081016] <p>"Frequency – This setting is used to prevent multiple alarms of the same state from the same device. Duplicate alarms will be ignored if they occur within the specified time period." (4-26) [SYM_P_0081024]</p> <p>"Alarms can be forwarded to another console. This is useful in complex networks where there is a hierarchical network management scheme using multiple consoles. A console monitoring a local network can pass status information on devices in its network to a master console. Selected alarms at the local console can be converted to traps and sent to another console." (4-28) [SYM_P_0081026]</p> |
| 2 | The method of claim 1, wherein integrating comprises correlating intrusion reports reflecting underlying commonalities. | See Figure 6-2 of NetStalker manual [SYM_P_0079597] | <p>"Automatically Acknowledging Alarms Generated by Traps The Acknowledge on Matching Trap and Variable text box allows you to clear a trap when a new specified trap is received. The original trap is moved from the current alarm log to the history alarm log. A variable in the trap packed that holds the network object's name can be selected to match the subobject field in the alarm log. This is to make sure that a trap that clears an alarm is referring to a particular device." (4-16) [SYM_P_0081014]</p> <p>"Frequency - This setting is used to prevent multiple alarms of the same state from the same device. Duplicate alarms will be ignored if they occur</p> |

NetStalker and HP OpenView

| Claim number | Claim Term | NetStalker (public use/on sale) | HP OpenView (printed publication and public use) within the specified time period.” (4-26) [SYM_P_0081024] |
|--------------|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3 | The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack. | <p>“Shun</p> <p>Blocks the source IP address from using the router. Be careful what is shunned. You may block yourself.” p. 6-16. [SYM_P_0079608]</p> <p>“For each alarm generated by <i>NetStalker</i>, you can configure one or more alarm handlers to serve as communications channels from <i>NetStalker</i> to you, to other network management tools or to respond to the alarm.” p. 4-2. [SYM_P_0079384]</p> | <p>“Configuring Alarms</p> <p>Applications monitor the state of network devices and processes and can trigger alarms. The alarms alert network managers of changes in the status of a device or group of devices. When an application detects a change in a device status, it can request OpenView to do one or more of the following:</p> <ul style="list-style-type: none"> • Change the device symbol to the new status color • Make an entry in the alarm log • Forward an alarm to another management console • Sound an alarm • Run a program” (4-21) [SYM_P_0081019] <p>“OpenView automatically logs an information alarm for each trap it receives. You can change OpenView’s default response to traps to sound an alarm, change color of the map symbol for the device sending the trap, or enter the trap in the alarm log. You can also change the default response to ignore traps from some or all devices, or configure one trap to auto-acknowledge another one when it is received.</p> <p>Each device class (hub type 1, hub type 2, router, server, etc.) can be assigned a different set of default and customized trap responses.” (4-11) [SYM_P_00811009]</p> <p>“Running Programs</p> <p>OpenView can run an MS-DOS or Windows program when an alarm is</p> |

NetStalker and HP OpenView

| 203 Claim number | Claim Term | NetStalker (public use/on sale) | HP OpenView (printed publication and public use) | | | | | | | | |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-------|-----------------------|----------|---------------|---------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools. | | generated. You can select what program is run based on the status of the alarm. Information about the alarm can be passed as command line arguments to the program." (4-29) [SYM_P_0081027] "In addition to running a program with a command line string, the alarm system can also pass information to another Windows application using DDE." (4-31) [SYM_P_0081029] "OpenView ships with the paging program <i>Notify</i> . <i>Connect</i> from Ex Machina Corporation. This program sends a paging message to a pager when a specified alarm goes off." (4-31) [SYM_P_0081029] | | | | | | | | |
| 4 | The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools. | <p>"Table 3 is a list of the actions that may take place when a datagram satisfies a pattern.</p> <p>Table 3. PCF Actions</p> <table><tr><th>Action</th><th>Parameters</th></tr><tr><td>alarm</td><td><i>severitynumber</i></td></tr><tr><td>clone_to</td><td><i>ipaddr</i></td></tr><tr><td>copy_to</td><td><i>ipaddr [portnum]"</i></td></tr></table> <p>Data Privacy Facility Administrator's Guide, DPF Version 1.2, Network Systems Corporation, 9/1995 at Appendix C page 197</p> | Action | Parameters | alarm | <i>severitynumber</i> | clone_to | <i>ipaddr</i> | copy_to | <i>ipaddr [portnum]"</i> | <p>"SNMP Manager</p> <p>The Simple Network Management Protocol (SNMP) Version 1.1 is a standard that defines a method of communicating with and controlling network devices. Devices that support the SNMP V.1 standard can be queried for their status and other device information. ... OpenView provides an SNMP Management function that can be used to communicate with SNMP devices. The device settings and other device information are available as variables and are defined either in a standard Management Information Base (MIB) file or in a custom MIB file provided by the device manufacturer." (1-7) [SYM_P_0080963]</p> <p>"A proxy agent is a device that acts on behalf of a device that does not have SNMP capabilities. The trap manager uses the Proxy Agent field." (4-2) [SYM_P_0081000]</p> |
| Action | Parameters | | | | | | | | | | |
| alarm | <i>severitynumber</i> | | | | | | | | | | |
| clone_to | <i>ipaddr</i> | | | | | | | | | | |
| copy_to | <i>ipaddr [portnum]"</i> | | | | | | | | | | |

NetStalker and HP Open View

| Claim number | Claim Term | NetStalker (public use/on sale) | HP Open View (printed publication and public use) |
|--------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 203 | | <p>"SNMP</p> <p>Simple Network Management Protocol - calls a shell to send an SNMP trap. The results of that trap is dependent on your site." p. 6-15. [SYM_P_0079607]</p> <p>"User Defined Alarms</p> <p>You can create up to three user-defined shells to activate unique alarm or response mechanisms for your site. The alarms can be as simple as sending a beep to the system console or more complex such as logging the event in syslog. ... When you turn on the user-defined alarm as explained in Chapter 5, <i>NetStalker</i> automatically calls the shell and supplies the complete data for the router event." pp. 4-5 to 4-6. [SYM_P_0079587- SYM_P_0079588]</p> | <p>"Configuring Alarms</p> <p>Applications monitor the state of network devices and processes and can trigger alarms. The alarms alert network managers of changes in the status of a device or group of devices. When an application detects a change in a device status, it can request OpenView to do one or more of the following:</p> <p>...</p> <ul style="list-style-type: none"> • Run a program" (4-21) [SYM_P_0081019] <p>"The SNMP Version 1 network devices store information about themselves in a Management Information Base (MIB). A MIB contains variables that describe the characteristics and current state of a network device. The SNMP Manager can access this information and control network devices that support SNMP." (5-1) [SYM_P_0081033]</p> <p>"The accessible SNMP variables are listed in the Variables box and may come from various MIBs. An extensive set comes with OpenView. Applications installed into OpenView may have added their own MIBs to the list. You may also use the MIB compiler to add MIBs." (5-3) [SYM_P_0081035]</p> <p>-----</p> <p>"This memo describes the common structures and identification scheme for the definition of management information used in managing TCP/IP-based internets. Included are descriptions of an object information model for network management along with a set of generic types used to describe</p> |

NetStalker and HP Open View

| Claim number | Claim Term | NetStalker (public use/on sale) | HP Open View (printed publication and public use) |
|--------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 203 | | | <p>management information. Formal descriptions of the structure are given using Abstract Syntax Notation One (ASN.1) [1].</p> <p>This memo is largely concerned with organizational concerns and administrative policy: it neither specifies the objects which are managed, nor the protocols used to manage those objects. These concerns are addressed by two companion memos: one describing the Management Information Base (MIB) [2], and the other describing the Simple Network Management Protocol (SNMP) [3].” (RFC 1155 p. 2) [SYM_P_0501013]</p> <p>“A collection of object types is defined in the MIB. Each such subject type is uniquely named by its OBJECT IDENTIFIER and also has a textual name, which is its OBJECT DESCRIPTOR.” (RFC 1155 p. 10) [SYM_P_0501021]</p> |
| 5 | The method of claim 1, wherein the enterprise network is a TCP/IP network. | <p>“NetStalker monitors all events reported from client NSC routers and PCF filters. Based on Haystack Labs’ patent pending technology, <i>NetStalker</i> automatically identifies network attacks and attempts to exploit TCP/IP protocol vulnerabilities in real using information stored in an internal database, the misuse signature database.” p. 1-2. [SYM_P_0079560]</p> | <p>“IP Discovery uses routers to discover and identify all IP devices in your network.” (2-2) [SYM_P_0080966]</p> <p>“This mask should be specific to your local network and also the same as the mask you specified when you installed your TCP/IP protocol stack.” (2-4) [SYM_P_0080968]</p> <p>-----</p> <p>“This memo describes the common structures and identification scheme for the definition of management information used in managing TCP/IP-based internets.” (RFC 1155 p.2) [SYM_P_0501013]</p> |
| 6 | The method of | “NetStalker monitors all events reported from client NSC | “To start a discovery, you need to know some information about your own |

NetStalker and HP Open View

| Claim number | Claim Term | NetStalker (public use/on sale) | HP Open View (printed publication and public use) |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3203 | claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}; | <p>routers and PCF filters. Based on Haystack Labs' patent pending technology, <i>NetStalker</i> automatically identifies network attacks and attempts to exploit TCP/IP protocol vulnerabilities in real using information stored in an internal database, the misuse signature database." p. 1-2. [SYM_P_0079560]</p> <p>"Before <i>NetStalker</i> can protect your network, you must configure the program for your site by setting up the routers to be monitored." p. 3-1 [SYM_P_0079577]</p> <p>"<i>NetStalker</i> has a standard set of named PCF filters that are used on NSC routers with router sensors to produce the messages used to communicate between the NSC router and <i>NetStalker</i>." p. 1-4. [SYM_P_0079562]</p> <p>"You add to the client list all the routers that this copy of <i>NetStalker</i> can monitor.</p> <p>To add a router, do the following:</p> <ol style="list-style-type: none"> 1. Deselect any client router names highlighted in the <i>NetStalker</i> window. 2. From the menu bar, select Configure; then select Client Information to display the Create New Client window. Use this window to enter all the client router information." p. 3-2. [SYM_P_0079578] | <p>network and the networks you want Autodiscovery to search. To run an IP discovery, you must provide the following information:</p> <p>...</p> <p>The IP address and community name for your default gateway or router if present." (2-2) [SYM_P_0080966]</p> <p>"Devices in the network are displayed on maps. Devices and subnetworks can be organized into submaps to suit your needs. You can create separate submaps of devices grouped by device function, network function, network organization, or corporate organization. You can use the maps to manage your network from a single display even when the network includes devices from different manufacturers. Programs that manage hubs, routers, servers, and other network devices can run in the background. Changes in network status are displayed on network maps with icons representing devices. Color is used to indicate device status. Submaps allow you to create several views of your network to simplify management. You can add meaningful graphics such as geographic maps and floor plans as backgrounds for your map to provide "real world" visual references for your network." (1-2) [SYM_P_0080958]</p> <p>"The Component symbol set contains various network components such as hubs, routers, and multiplexers. Open View applications can add symbols or delete symbols from the standard set." (3-14) [SYM_P_0080996]</p> <p>-----</p> <p>"Implicit in the SNMP architectural model is a collection of network</p> |

NetStalker and HP Open View

| Claim number | Claim Term | NetStalker (public use/on sale) | HP OpenView (printed publication and public use) |
|--------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 203 | | <p>“Network</p> <p>The Network filter queries events based on the origin or destination of the connection to the router using the network address for internal or external connections. Network addresses contain the individual addresses, the classes of the addresses, and sets of individuals/classes.” p. 6-10. [SYM_P_0079602]</p> <p>“Types</p> <p>Events</p> <p>The Events filters query the router events based on router event types or PCF filters installed at the router.</p> <p>The Event Types filter examines the data for specific events or classes of events. When you select Event Types, the Configure Event Types window is displayed (Figure 6-11). Ten event classes are listed, of which nine are for router events and one is for PCF filter events. For more information about router event types, see the NSC manual for your router.” p. 6-12. [SYM_P_0079604]</p> <p>“Initial PC Filter Configuration</p> | <p>management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements.” (RFC 1157 p. 4) [SYM_P_0527111]</p> <p>“Upon receiving a subtree, the enterprise may, for example, define new MIB objects in this subtree. In addition, it is strongly recommended that the enterprise will also register its networking subsystems under this subtree, in order to provide an unambiguous identification mechanism for use in management protocols. For example, if the “Flintstones, Inc.” enterprise produced networking subsystems, then they could request a node under the enterprises subtree from the Internet Assigned Numbers Authority. Such a node might be numbered:</p> <p>1.3.6.1.4.1.42</p> <p>The “Flintstones, Inc.” enterprise might then register their “Fred Router” under the name of:</p> <p>1.3.6.1.4.1.42.1.1” (RFC 1155 p. 6) [SYM_P_0501017]</p> |

NetStalker and HP OpenView

| Claim number | Claim Term | NetStalker (publicuse/on sale) | HP OpenView (printed publication and public use) |
|--------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 203 | | <p><i>NetStalker</i> has a standard set of named PCF filters that are used on NSC routers with router sensors to produce the messages used to communicate between the NSC router and <i>NetStalker</i>. The filters are created and downloaded to the router when you run the shell, INSTALL.filters. See Chapter 2 for information on installing <i>NetStalker</i>. " p. 1-4. [SYM_P_0079562]</p> <p>"Securing the Connection</p> <p>Since the <i>Netstalker</i> server platform can be located anywhere on the network, there is the potential of an attacker manipulating the connection between the router and the <i>NetStalker</i> server platform.</p> <p>The most efficient means of protecting this connection between the NSC router client and the <i>NetStalker</i> is to use separate BorderGuard routers between the <i>NetStalker</i> platform and the network, and then to configure an encrypted tunnel between the client router and the "guard" router that protects the <i>NetStalker</i> platform. Since all IP traffic between the <i>NetStalker</i> platform and client is encrypted on the network, the encryption provides confidentiality, integrity, and mutual authentication of the communicating parties.</p> | <p>"See also the Host and Gateway Requirements RFCs for more specific information on the applicability of this standard." (RFC 1155 p. 1) [SYM_P_0501013]</p> <p>"sysServices OBJECT-TYPE layer functionality 1 physical (e.g., repeaters) 2 datalink/subnetwork (e.g., bridges) 3 internet (e.g., IP gateways) 4 end-to-end (e.g., IP hosts) 7 applications (e.g., mail relays)</p> <p>For systems including OSI protocols, layers 5 and 6 may also be counted." (RFC 1213 p. 14) [SYM_P_0501155-SYM_P_0501156]</p> <p>"ipForwarding OBJECT-TYPE SYNTAX INTEGER { forwarding(1), -- acting as a gateway not-forwarding(2) -- NOT acting as a gateway }" (RFC 1213 p. 25) [SYM_P_0501165]</p> <p>"Remote network monitoring devices are instruments that exist for the purpose of managing a network. Often these remote probes are stand-alone devices ... An organization may employ many of these devices, one per</p> |

NetStalker and HP OpenView

| Claim number | Claim Term | NetStalker (public use/on sale) | HP OpenView (printed publication and public use) |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 203 | | <p>Alternatively, the <i>NetStalker</i> platform can be located on an individual network segment that is directly connected to a dedicated port on the router it is monitoring." p. 1-4. [SYM_P_0079562]</p> <p>"Before <i>Netstalker</i> can protect your network, you must configure the program for your site by setting up the routers to be monitored. This chapter describes how to add and edit client routers listed in the <i>NetStalker</i> window. It also describes how to verify the client information..." pp. 3-1-3-6. [SYM_P_0079577-SYM_P_0079582]</p> | <p>network segment, to manage its internet." (RFC 1271 p. 3) [SYM_P_0501208]</p> <p>See Figure 12 in my expert report.</p> |
| 7 | The method of claim 1, wherein the network monitors plurality of service monitors among multiple domains of the enterprise network. | <p>"Before <i>NetStalker</i> can protect your network, you must configure the program for your site by setting up the routers to be monitored." p. 3-1. [SYM_P_0079577]</p> <p>"<i>NetStalker</i> has a standard set of named PCF filters that are used on NSC routers with router sensors to produce the messages used to communicate between the NSC router and <i>NetStalker</i>." p. 1-4. [SYM_P_0079562]</p> <p>"You add to the client list all the routers that this copy of <i>NetStalker</i> can monitor.</p> <p>To add a router, do the following:</p> | <p>"Before you create a network map, you need to know the physical layout of your network. It may be a single LAN, several LANs, or a very complex enterprise-wide network. Whenever possible you should break your map into submaps that help you visualize the network organization. You can create submaps for a workgroup, building site, device type, or any other convenient grouping. The same device can be placed on several submaps to provide alternate "views" of the network. ... The submap symbol displays the most severe status color for all of the nodes or devices within it. This allows the most severe status information for any device in the network to be propagated up to the home submap. The home submap can then give you an overview of status for the entire network." (3-2) [SYM_P_0080984]</p> |

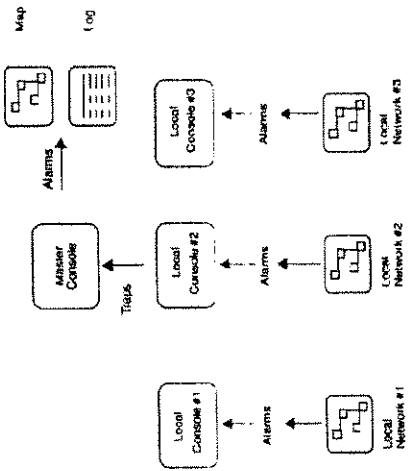
NetStalker and HP OpenView

| Claim number | Claim Term | NetStalker (public use/on sale) | HP OpenView (printed publication and public use) |
|--------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 243 | | <p>1. Deselect any client router names highlighted in the <i>NetStalker</i> window.</p> <p>2. From the menu bar, select Configure; then select Client Information to display the Create New Client window. Use this window to enter all the client router information.” p. 3-2. [SYM_P_0079578]</p> | <p>“Figure 4-2 Map set to propagate alarms up all levels.”</p> <p>“Normally, you would select to propagate up all levels. Then, if your home submap contains a submap symbol for each submap in the next lower level in the map, you can check your network’s overall status from the home submap. If a submap represents several devices, its submap symbol on the</p> |

NetStalker and HP OpenView

| 203 Claim number | Claim Term | NetStalker (public use/on sale) | HP OpenView (printed publication and public use) |
|------------------------|------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | <p>home submap will display the most severe device status for the lower submap.” (4-19) [SYM_P_0081017]</p> <p>“Alarm Forwarding Alarms can be forwarded to another console. This is useful in complex networks where there is a hierarchical network management scheme using multiple consoles. A console monitoring a local network can pass status information on devices in its network to a master console. Selected alarms at the local console can be converted to traps and sent to another console.” (4-28) [SYM_P_0081026]</p> |

NetStalker and HP OpenView

| Claim number | Claim Term | NetStalker (public use/on sale) | HP OpenView (printed publication and public use) |
|--------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8 | The method of claim 7, wherein receiving and integrating is performed by a domain monitor | <p>"Before <i>NetStalker</i> can protect your network, you must configure the program for your site by setting up the routers to be monitored." p. 3-1. [SYM_P_0079577]</p> <p>"<i>NetStalker</i> has a standard set of named PCF filters that are used on NSC routers with router sensors to produce the</p> |  <p>(4-28) [SYM_P_0081026]</p> <p>See Figure 12 in my expert report.</p> <p>"Before you create a network map, you need to know the physical layout of your network. It may be a single LAN, several LANs, or a very complex enterprise-wide network. Whenever possible you should break your map into submaps that help you visualize the network organization. You can create submaps for a workgroup, building site, device type, or any other convenient grouping. The same device can be placed on several submaps to</p> |

NetStalker and HP Open View

| 203 Claim number | Claim Term | NetStalker (public use/on sale) | HP OpenView (printed publication and public use) |
|------------------------|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | with respect to a plurality of service monitors within the domain monitor's associated network domain. | <p>messages used to communicate between the NSC router and <i>NetStalker</i>." p. 1-4. [SYM_P_0079562]</p> <p>"You add to the client list all the routers that this copy of <i>NetStalker</i> can monitor.</p> <p>To add a router, do the following:</p> <ol style="list-style-type: none"> 1. Deselect any client router names highlighted in the <i>NetStalker</i> window. 2. From the menu bar, select Configure; then select Client Information to display the Create New Client window. Use this window to enter all the client router information." p. 3-2. [SYM_P_0079578] | <p>provide alternate "views" of the network. ... The submap symbol displays the most severe status color for all of the nodes or devices within it. This allows the most severe status information for any device in the network to be propagated up to the home submap. The home submap can then give you an overview of status for the entire network." (3-2)</p> <p>[SYM_P_0080984]</p> |

NetStalker and HP OpenView

| Claim number | Claim Term | NetStalker (public use/on sale) | HP OpenView (printed publication and public use) |
|--------------|------------|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 203 | | | <div><p>World - "Home Submap"</p><p>U.S.A. Europe Japan</p><p>San Jose Dallas New York</p><p>Legend: ○ = Normal ◐ = Warning ● = Critical</p></div> <p>Figure 4-2 Map set to propagate alarms up all levels.</p> <p>Normally, you would select to propagate up all levels. Then, if your home submap contains a submap symbol for each submap in the next lower level in the map, you can check your network's overall status from the home submap. If a submap represents several devices, its submap symbol on the home submap will display the most severe device status for the lower</p> |

NetStalker and HP Open View

| 203 Claim number | Claim Term | NetStalker (public use/on sale) | HP Open View (printed publication and public use) |
|------------------------|------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | <p>submap. (4-19) [SYM_P_0081017]</p> <p>“Alarm Forwarding Alarms can be forwarded to another console. This is useful in complex networks where there is a hierarchical network management scheme using multiple consoles. A console monitoring a local network can pass status information on devices in its network to a master console. Selected alarms at the local console can be converted to traps and sent to another console.” (4-28) [SYM_P_0081026]</p> <p>The diagram illustrates an alarm forwarding architecture. At the top, a 'Master Console' is connected to three 'Local Consoles' (Local Console #1, Local Console #2, and Local Console #3). Each local console is connected to a corresponding 'Local Network' (Local Network #1, Local Network #2, and Local Network #3). Arrows labeled 'Alarms' point from each local console to the master console. An arrow labeled 'Traps' points from the master console to a 'Map' icon. A 'Log' icon is also shown. The diagram is labeled (4-28).</p> |

NetStalker and HP Open View

| 203 Claim number | Claim Term | NetStalker (public use/on sale) | HP OpenView (printed publication and public use) |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| 9 | The method of claim 1, wherein network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network. | <p><u>103</u></p> <p>"The next step in creating a custom misuse detection configuration to select one or more alarms and to assign the parameters for triggering the alarm.</p> <p>In the Configure Alarm Handler window, you created the alarm configurations (See Chapter 4). In the Configure Misuse Detector window, you activate the alarms for specified Misuse Detector configurations.</p> <p>To activate an alarm, select the alarm type from the displayed list." p. 6-15. [SYM_P_0079607]</p> <p>See "Alarm Types" pp. 6-15 to 6-17: [SYM_P_0079607-SYM_P_0079609]</p> <p>"SNMP</p> <p>Simple Network Management Protocol - calls a shell to send an SNMP trap. The results of that trap is dependent on your site." p. 6-15. [SYM_P_0079607]</p> | <p>[SYM_P_0081026]</p> <p>See Figure 12 in my expert report.</p> <p>See '203 claim 8</p> <p>See Figure 12 in my expert report.</p> |
| 10 | The method of | See '203 claim 9 | See '203 claim 8 |

NetStalker and HP OpenView

| 203 Claim number | Claim Term | NetStalker (public use/on sale) | HP OpenView (printed publication and public use) |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | claim 9, wherein receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network. | | <p>"Alarm Forwarding Alarms can be forwarded to another console. This is useful in complex networks where there is a hierarchical network management scheme using multiple consoles. A console monitoring a local network can pass status information on devices in its network to a master console." (4-28) [SYM_P_0081026]</p> |
| 12 | An enterprise network monitoring system comprising: | See '203 claim 1 | See '203 claim 1 |
| | a plurality of network monitors deployed within an enterprise network; | See '203 claim 1 | See '203 claim 1 |
| | said plurality of network monitors detecting suspicious network activity | See '203 claim 1 | See '203 claim 1 |
| | based on analysis of network traffic data selected from the following categories: {network packet data transfer | See '203 claim 1 | See '203 claim 1 |

NetStalker and HP Open View

| Claim number | Claim Term | NetStalker (public use/on sale) | HP Open View (printed publication and public use) |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|------------------------------------------------------|
| 203 | commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}; | | |
| | said network monitors generating reports of said suspicious activity; and | See '203 claim 1 | See '203 claim 1 |
| | one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity. | See '203 claim 1 | See '203 claim 1 |
| 13 | The system of claim | | See '203 claim 2 |

NetStalker and HP OpenView

| '203 Claim number | Claim Term | NetStalker (public use/on sale) | HP OpenView (printed publication and public use) |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|-----------------------------------------------------|
| | 12, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities. | | |
| 14 | The system of claim 12, wherein the integration further comprises invoking countermeasures to a suspected attack. | See '203 claim 3 | See '203 claim 3 |
| 15 | The system of claim 12, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools. | See '203 claim 4 | See '203 claim 4 |
| 16 | The system of claim 12, wherein the | See '203 claim 5 | See '203 claim 5 |

NetStalker and HP Open View

| 203 Claim number | Claim Term | NetStalker (public use/on sale) | HP Open View (printed publication and public use) |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|------------------------------------------------------|
| | enterprise network is a TCP/IP network. | | |
| 17 | The system of claim 12, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}. | See '203 claim 6 | See '203 claim 6 |
| 18 | The system of claim 12, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network. | See '203 claim 7 | See '203 claim 7 |
| 19 | The system of claim 18, wherein a domain monitor associated with the | See '203 claim 8 | See '203 claim 8 |